УДК 343.85

П. Н. Кобец
главный научный сотрудник
Всероссийского научно-исследовательского института МВД России,
доктор юридических наук, профессор

ВАЖНОСТЬ УГОЛОВНО-ПРАВОВОЙ ОЦЕНКИ ДЛЯ ЭФФЕКТИВНОЙ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

В условиях третьего десятилетия XXI столетия в общественном понимании широко распространено утверждение о том, что киберпреступления развиваются также стремительно, как и кибертехнологии. Между тем важно отметить, что в современном российском уголовном законодательстве отсутствует четкое определение киберпреступности. В то же время рост противоправных посягательств в киберпространстве способствовал возникновению целого комплекса криминологических понятий, которые характеризуют рассматриваемую преступность. Поэтому в настоящее время в юридической литературе преступления, совершенные в сфере киберпространства, различные исследователи и специалисты называют по-разному, в частности компьютерными преступлениями, противоправными деяниями, совершенными в киберпространстве, киберсфере и др. Одним словом, сегодня чрезвычайно широко распространяется применение определений, под которыми понимаются похожие действия, которые совершаются в киберпространстве. Как правило, многие исследователи к ним пытаются отнести преступные посягательства в области электронной информации [1, с. 37], компьютерной сферы [2, с. 85], в области информбезопасности и информтехнологий [3, с. 75], кибертехнологий [4, с. 93], компьютерной преступности [5, с. 30] и др.

Российским уголовным законодательством, в частности его двадцать восьмой главой, регламентируется ответственность только за совершение противоправных деяний в сфере компьютерной информации [6, с. 101]. И как полагают многие российские специалисты, в современных условиях данные законодательные нормы просто не адаптируются ко многим видам преступных посягательств, совершаемых в киберсфере [7, с. 45]. А реальная оптимизация правоприменительной работы по расследованию киберпреступных посягательств будет только тогда, когда активизируется нормотворческая деятельность в рассматриваемом направлении. Поэтому в сложившейся ситуации следовало бы согласиться с мнением ряда российских экспертов, в соответствии с которым эффективное противостояние киберпреступным проявлениям возможно только при наличии адекватных правовых международных и национальных мер

в рассматриваемой сфере, которые не будут тормозить расследование, а также принятие судебных решений по наказанию виновных в совершении преступлений в киберсфере [8, с. 49].

А пока что в сложившейся ситуации в системе современного права правоохранителям, давая уголовно-правовую оценку киберпреступлениям, довольно непросто квалифицировать уголовно-правовые составы, которые предстоит им расследовать. Ученые, правоведы так же, как и практики, ощущая недостаточность законодательного регулирования борьбы с киберпреступностью, которое бы в полной мере отвечало всем требуемым потребностям правоприменения, не имеют возможности полной и объективной оценки тех масштабов правонарушений, которые обусловлены киберпреступностью [9, с. 141].

Также важно отметить, что отдельными специалистами выделены некоторые специфические особенности, характерные для преступных проявлений в киберпространстве, на основе которых возможно проводить классификацию обозначенных противоправных деяний на основе следующих оснований: средства и способы совершения преступлений, цели, объект и субъект рассматриваемых преступных посягательств [10, с. 255]. К средствам рассматриваемых преступных деяний, как правило, относят компьютерную технику, различные компьютерные системы, мобильную телефонию, цифровые носители, компьютерные приборы, гаджеты и др.

Ежегодно информтехнологии все активнее распространяются среди граждан, поскольку сетевые системы постоянно развиваются, чем и затрудняют процессы по законодательному закреплению ответственности за различные способы совершения киберпреступлений. Также, помимо недостаточно проработанного правового регулирования в сфере противодействия киберпреступности, важнейшей из дальнейших задач является повышение профессиональной подготовленности субъектов борьбы с рассматриваемым феноменом.

В свете вышесказанного можно утверждать о том, что проблематика, связанная со сложной уголовно-правовой оценкой киберпреступных проявлений, по большей части в настоящее время обусловлена в недостаточной степени проработанной законодательной основой уголовно-правовых составов по борьбе с киберпреступностью, различными сложностями по сбору доказательственной базы киберпреступлений и, конечно, непростой ситуацией при доказывании рассматриваемых противоправных деяний.

Список основных источников

1. Головко Д. И. Квалификация преступлений в сфере электронной информации, совершенных группой лиц по предварительному сговору и организованной

преступной группой // Юрид. вестн. Ростов. гос. эконом. ун-та. 2011. № 59. С. 36–39. Вернуться к статье

2. Сретенцев А. Н., Казаков А. В. Некоторые особенности расследования преступления в сфере компьютерной информации // Науч. вестн. Орлов. юрид. ин-та МВД России им. В. В. Лукьянова. 2020. № 4 (85). С. 84–89. Вернуться к статье

3. Кириллова Н. П., Кушниренко С. П. Проблемы осуществления уголовного преследования по делам о преступлениях, совершаемых в сфере высоких информационных технологий // Изв. высш. учеб. заведений. Правоведение. 2013. № 3 (308). С. 74–90. Вернуться к статье

4. Кобец П. Н. Причины и тенденции киберугроз, возникающих в экономической сфере, и комплекс мер по их нейтрализации // Науч. вестн. Орлов. юрид. ин-та МВД России им. В. В. Лукьянова. 2022. № 3 (92). С. 93–101. Вернуться к статье

5. Китайкина О. О. О соотношении понятий «компьютерные преступления» и «преступления в сфере компьютерной информации» // Научный формат. 2020. № 8 (11). С. 29–36. Вернуться к статье

6. Кобец П. Н. Основы обеспечения национальной экономической безопасности от новейших угроз киберпреступности // Научное обозрение: теория и практика. 2022. Т. 12. № 3 (91). С. 426–434. Вернуться к статье

7. Козлова О. Е., Самойлова А. В., Твердохлебова Э. В. Перспективы применения положительного опыта зарубежных стран в борьбе с киберпреступностью в Российской Федерации // Актуальные научные исследования в современном мире. 2020. № 8-5 (64). С. 42–47. Вернуться к статье

8. МСЭ делает информационную среду безопасной // Век качества. 2011. № 6. С. 48–50. Вернуться к статье

9. Жуков А. З. Киберпреступность: актуальные проблемы и уголовно-правовая оценка в системе современного права // Проблемы экономики и юридической практики. 2019. Т. 15. № 4. С. 141–143. Вернуться к статье

10. Куява Т. Ю. Киберпреступность: проблемы уголовно-правовой оценки и организации противодействия // Молодой ученый. 2016. № 29 (133). С. 255–257. Вернуться к статье